UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/815,396	03/31/2004	Christopher J. Lord	110466-152116	7579

31817 7590 09/29/2009
SCHWABE, WILLIAMSON & WYATT, P.C.
PACWEST CENTER, SUITE 1900
1211 S.W. FIFTH AVE.
PORTLAND, OR 97204

EXAMINER	
ZHANG, SHIRLEY X	

ART UNIT	PAPER NUMBER
2444	

MAIL DATE	DELIVERY MODE
09/29/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/815,396	**Applicant(s)** LORD ET AL.
	Examiner SHIRLEY X. ZHANG	**Art Unit** 2444

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 June 2009*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8,9,11 and 23-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-9, 11, 23-31* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Claims 1-9, 11-14, 16-32 and 34-35 were previously pending in the final action mailed on April 1, 2009.

In the amendments filed on June 30, 2009,

Claims 7, 12-14, 16-22, 32, 34-35 are cancelled;

Claims 1, 23 and 27 are amended;

Claims 1-6, 8-9, 11 and 23-31 are now pending.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on June 30, 2009 has been entered.

Response to Amendments

2. Applicant's arguments and amendments filed on June 30, 2009 have been carefully considered and new grounds of rejection are introduced in this action to better address the claimed invention in its current form.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. **Claims 27-31** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 27 recites "an article of manufacture comprising a storage medium."

Applicant states in the specification in the specification (U.S. PG-Pub 2005/0240758, paragraph [0049]) that

"the invention may be described by reference to associated data including functions, procedures, data structures, application programs, etc.", which means that the invention may be described as software or data structures.

Applicant further states in the specification (U.S. PG-Pub 2005/0240758, paragraph [0049]) that

"Associated data may be delivered over transmission environments, including network 422, in the form of packets, serial data, parallel data, propagated signals, etc."

leading one skilled in the art into concluding that the associated data, i.e., software, may be stored in a transmission environment, therefore the storage medium could be a transmission environment".

Computer programs claimed as computer listings per se, i.e., the descriptions or expressions of the programs are not physical "things". They are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed elements of a computer, which permit the computer program's functionality to be realized.

MPEP 2601.1 Section I states, "Since a computer program is merely a set of instructions capable of being executed by a computer, the computer program itself is not a process and USPTO personnel should treat a claim for a computer program, without the computer-readable medium needed to realize the computer program's functionality, as nonstatutory functional descriptive material."

Furthermore, an article of manufacture comprising storage medium that could be in the form of a propagated signal means that the article of manufacture could be a propagated signal, which is non-patentable subject matter.

Claims 28-31 are dependent on claim 27, but fail to further limit claim 27 to statutory subject matter, therefore inherit the 35 U.S.C. 101 issue of the independent claim.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 3 recites the limitation "the UPnP Simple Service Discovery Protocol (SSDP)." There is insufficient antecedent basis for this limitation in the claim.

5. Claim 25 recites the limitation "the UPnP Security Protocol." There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 1-2, 9, 11, 23-24, 27-28 and 31** are rejected under 35 U.S.C. 103(a) as obvious over Kadyk et al. (U.S. 2002/0157019, hereinafter "Kadyk"), in view of Crosbie (U.S. U.S. 2002/0035699).

Regarding claim 1, Kadyk disclosed a method for an intermediary selectively coupling an external network and an internal network to dynamically generate filter rules to facilitate establishing an end to end secure session connection between a first device on the internal network and a second device of the external network, the method comprising:

receiving a secure session establishment request by the second device on the external network to establish a secure communication session with the first device on the internal network (Kadyk, Fig. 4 and [0053] disclosed that "The step for negotiating a secure end-to-end connection may include the acts of client 402 sending a request to proxy 404 for the secure end-to-end connection", where the "client 402" anticipates "the second device" in the claim, and "server 406" anticipates "the first device");

forwarding the secure session establishment request to the first device (Kadyk, Fig. 4 and [0055] disclosed that "the proxy 404 performs the act of forwarding the request for a secure end-to-end connection to the server or cascaded proxy 406");

monitoring the internal network to detect an approval or disapproval acknowledgement by the first device for the secure session establishment request (Kadyk, [0044] disclosed that "when server 204a receives request 212 for the protected page, server 204a checks the permissions required for the page and rejects (220) request 212 because the proper credentials were not included with the request." Although this Kadyk did not explicitly disclose that the rejection of a request is done in the same embodiment as the one shown in Fig. 4, but Kadyk disclosed in the first sentence of [0056] that the server 406 issues authenticate challenges to client 404. The disclosures combined would have made it obvious to one skilled in the art that that the result of the authentication could be either an approval or a disapproval); and

configuring a first filter rule of the intermediary to allow communication between the first and second devices through the intermediary, if an approval authentication acknowledgement is detected (Kadyk, Fig. 4 and [0056] disclosed that if the server 406 authenticates the client 404, a secure end-to-end connection between the client 402 and server 406 is established and the secure end-to-end connection is encapsulated within the insecure client-proxy connection);

Kadyk did not explicitly disclose

determining whether network traffic from the second device is corresponding to a previous secure communication session established when the second device was previously on the internal network, wherein the second device uses an address that is globally routable on the internal and the external networks and therefore said network traffic is valid with respect to the internal network; and responding to said network traffic with an error and forcing the second device to re-establish a secure communication session from the external network.

However, Crosbie disclosed that in a system where mobile devices connect to protected by Gateway Server and Firewall (Crosbie, Fig. 1), the mobile device is typically re-required to re-establish a stateful end to end connection such as IPSec (Crosbie, [0008]), which is essentially what the above cited claim elements try to do.

One of ordinary skill in the art would have been motivated to combine Kadyk and Crosbie because both disclosed establishing a secure end-to-end connection between a client device in a first network and a server in a second network (Kadyk, Fig. 4; Crosbie, Fig. 1).

Therefore, it would have been obvious for one skilled in the art to combine Kadyk and Crosbie's teaching to realize that if the client device in Kadyk were a roaming mobile that moved outside its previous network, the secure end-to-end would have to be re-established.

Claim 27 lists substantially the same elements of **claim 1**, but in product form rather than method form. Therefore, the supporting rationale of the rejection to **claim 1** applies equally as well to **claim 27**.

Regarding claims 2 and 28, the combination of Kadyk and Crosbie disclosed the method of claims 1 and 27.

Kadyk did not explicitly disclose determining a presence advertisement for the first device has been received before forwarding the secure session establishment request to the first device.

However, in the same field of endeavor, Moyer disclosed a system that uses SIP to communicate with appliances in a private home network through a firewall/proxy, where the proxy maintains a location database 140 that contains location information for all appliances that send a REGISTER message to the proxy to announce its location (e.g. address) (Moyer, [0094]). Moyer further disclosed that the proxy resolves the address of the appliance to be communicated with (including the appropriate Home domain RGW) by means of a lookup in the location database 140. The proxy then forwards appliance messages from the Client SIP UA 100 to the SIP Proxy 116' in the Home Domain RGW or, via a secure connection, directly to the SIP UAS in the target device (Moyer, [0093]).

Moyer's disclosure is essentially the same as "determining a presence advertisement for the first device has been received before forwarding the secure session establishment request to the first device."

One of ordinary skill in the art would have been motivated to combine Kadyk and Moyer because both disclosed establishing a secure end-to-end connection between a client device in a first network and a server in a second network through a proxy/firewall (Kadyk, Fig. 4; Moyer, Fig. 3).

Therefore, it would have been obvious for one to apply Kadyk's teaching of a general purpose method for creating end-to-end secure session using any protocols to Moyer's specific system for using SIP to control home appliances in a private network from a public network to achieve end-to-end security that is suggested by Moyer in [0453] for the highly desirable result of achieving privacy.

Regarding claims 9 and 31, the combination of Kadyk and Crosbie disclosed the method of claims 1 and 27.

Kadyk further disclosed

retrieving an Access Control List (ACL) from the first device, the ACL including an identification of devices authorized to establish communication sessions; and determining based at least in part on the ACL the second device is authorized to establish the secure communication session with the first device before forwarding the secure session establishment request to the first device (Kadyk, Fig. 4 and [0054] disclosed the process a proxy take to authenticate a client, which implies that the proxy must have an access control list identifying the client devices that are authorized access so that the proxy can check a requesting client against the list to verify the client's credential).

Regarding claim 11, the combination of Kadyk and Crosbie disclosed the method of claims 1 and 27.

Kadyk further disclosed establishing the end to end secure session connection between the first device on the internal network and the second device of the external network in a single end to end secure session connection between said first and second devices (Kadyk, Fig. 4, reference 450).

Claim 23 lists substantially the same elements of **claim 1**, but in system form rather than method form. Therefore, the supporting rationale of the rejection to **claim 1** applies equally as well to **claim 23**.

Regarding claim 24, the combination of Kadyk and Crosbie disclosed the method of claim 23.

Kadyk further disclosed wherein the intermediary is further configured to monitor the first device for an approval or disapproval authentication acknowledgement for the request Kadyk, [0044] disclosed that "when server 204a receives request 212 for the protected page, server 204a checks the permissions required for the page and rejects (220) request 212 because the proper credentials were not included with the request." Although this Kadyk did not explicitly disclose that the rejection of a request is done in the same embodiment as the one shown in Fig. 4, but Kadyk disclosed in the first sentence of [0056] that the server 406 issues authenticate challenges to client 404. The disclosures combined would have made it obvious to one skilled in the art that that the result of the authentication could be either an approval or a disapproval), and

to configure a filter of the intermediary controlling communication over the first network from the first device based at least in part on a monitored authentication acknowledgement (Kadyk, Fig. 4 and [0056] disclosed that if the server 406 authenticates the client 404, a secure end-to-end connection between the client 402 and server 406 is established and the secure end-to-end connection is encapsulated within the insecure client-proxy connection).

7. **Claim 3** is rejected under 35 U.S.C. 103(a) as obvious over Kadyk and Crosbie, further in view of Moyer et al.(U.S. 2002/0103898, hereinafter "Moyer").

Regarding claim 3, the combination of Kadyk and Crosbie disclosed the method of claim 2.

Kadyk did not explicitly disclose wherein the presence advertisement is delivered in accordance with the UPnP Simple Service Discovery Protocol (SSDP).

However, Moyer disclosed a device messaging protocol (DMP) and explicitly states that it is similar to universal plug n play (UPnP) Device Control Protocol, making it clearly that at the time the invention was made, it was well within the knowledge of one skilled in the art that UPnP can be used to control appliances in a home network.

The rationale for combining Kadyk and Moyer is the same as that provided above for the rejection of claim 2.

As UPnP Simple Service Discovery Protocol (SSDP) is the protocol in UPnP framework for discovering device, which serves the same purpose as SIP REGISTER, it would have been obvious for one to substitute UPnP for SIP in Moyer to achieve the same result. Such modification, along with the combination of Kadyk and Moyer, would have resulted in a remote home appliance control system using UPnP with end-to-end security.

8. **Claims 4-6 and 29-30** are rejected under 35 U.S.C. 103(a) as obvious over Kadyk and Crosbie, further in view of Cho (U.S. 2003/0217136).

Regarding claim 4, the combination of Kadyk and Crosbie disclosed the method of claim 1.

Kadyk did not explicitly disclose receiving network traffic from the second device corresponding to the second device requesting a UPnP Device Description Document from the first device.

However, in a system for controlling appliances in an internal network from an external network, Cho disclosed using UPnP and receiving network traffic from the second device corresponding to the second device requesting a UPnP Device Description Document from the first device (Cho, Fig. 7 and [0071] disclose that upon receiving a service description request message from the stub 102 (step 717), the agent 131 sends the received message to the bridge 132 (step 718), which then transfers it to the specific UPnP device (step 719)).

One of ordinary skill in the art would have been motivated to combine Kadyk and Cho because both disclosed accessing devices in an internal network from a device in an external Internet via a proxy(Kadyk, Fig. 4; Cho, Fig. 1).

Therefore, it would have been obvious for one to apply Kadyk's teaching of a general purpose method for creating end-to-end secure session using any protocols to Cho's system to achieve the desirable result of securing the communications between Cho's wired/wireless internet client and UPnP home devices such that the UPnP devices will not be tempered by malicious clients from the internet.

Regarding claims 5, 29, the combination of Kadyk, Crosbie disclosed the subject matter of claims 1 and 27, respectively.

Kadyk did not explicitly disclose but Cho further disclosed:

receiving a service request from the second device for the first device, the service request having an associated communication port for performing the service (Cho, Fig. 7, "device control command 729"; Cho, [0044] further disclosed that the message processing module on the UPnP Proxy conducts communications according to HTTP protocol; As HTTP is a TCP based protocol, a service request such as the "device control command" inherently has an associated communication port);

determining the service request identifies a service advertised by the first device in a device description document (Cho, Fig. 7 and [0040]); and

configuring a second filter rule to allow communication between the first device and the second device using the associated communication port (Cho, [0007] disclosed that a home network can be a private network and [0008] disclosed using NAT; For NAT, a filter rule must exist in the proxy device to translate between the public IP address and private IP address to allow communication between home network and Internet).

The rationale for combining Kadyk and Cho is the same as that provided above for the rejection of claim 4.

Regarding claims 6 and 30, the combination of Kadyk and Crosbie disclosed the subject matter of claims 1 and 27, respectively.

Kadyk did not explicit disclose but Cho further disclosed that the method comprises:

providing the second device with an indicia for use by the second device in establishing a communication link to the first device (Cho, Fig.7 and [0071] disclose that the specific UPnP device sends the service description to the bridge 132 (720), which then transfers it to the agent 131 (721), where the service description is equivalent to the indicia recited in the claim).

The rationale for combining Kadyk and Cho is the same as that provided above for the rejection of claim 4

9. **Claims 25-26** are rejected under 35 U.S.C. 103(a) as obvious over Kadyk and Crosbie, further in view of Cho (U.S. 2003/0217136) and the article "UPnP™ Security Ceremonies Design Document For UPnP Device Architecture 1.0" authored by Ellison and published by the UPnP Forum (hereinafter "**Ellison**").

Regarding claim 25, the combination of Kadyk and Crosbie disclosed the system of claim 23.

Kadyk did not explicit disclose wherein the first device communicates with the second device in accord with the UPnP Security Protocol.

However, disclosed that the first device communicates with the second device in accord with the UPnP Security Protocol (Cho, Fig. 1 and "Abstract" disclosed using UPnP framework to control devices in an internal network from a device in an external network).

However, Cho disclose a UPnP-based system for controlling appliances in an internal network from an external network (Cho, Fig. 1 and "Abstract"), while Ellison disclosed a UPnP security protocol, for a UPnP system.

One of ordinary skill in the art would have been motivated to combine Kadyk and Cho because both disclosed accessing devices in an internal network from a device in an external Internet via a proxy(Kadyk, Fig. 4; Cho, Fig. 1).

Therefore, it would have been obvious for one skilled in the art to combine Kadyk's teaching of a general purpose method for creating end-to-end secure session using any protocols with Cho's teaching of a UPnP framework for controlling UPnP compatible home appliances and realize that the UPnP security protocol disclosed by Ellison is an obvious choice for Cho's security needs.

Regarding claim 26, the combination of Kadyk and Crosbie disclosed the system of claim 23.

Kadyk did not explicitly disclose that the secure communication initiation request corresponds to a UPnP Set Session Key (SSK) request.

However, Cho disclose a UPnP-based system for controlling appliances in an internal network from an external network (Cho, Fig. 1 and "Abstract"), while Ellison disclosed a UPnP security protocol for an UPnP system, where a UPnP Set Session Key (SSK) request is used to initiate a secure communication (Ellison, page 13, section 5, "Session Keys")

Therefore, it would have been obvious for one skilled in the art to combine Kadyk's teaching of a general purpose method for creating end-to-end secure session using any protocols with Cho's teaching of a UPnP framework for controlling UPnP compatible home appliances and realize that the UPnP security protocol disclosed by Ellison is an obvious choice for Cho's security needs.

---

10. **Claim 8** is rejected under 35 U.S.C. 103(a) as being unpatentable over Kadyk and Crosbie as applied to claim 1 above, further in view of Le et al. (U.S. 2005/0111382, hereinafter "**Le**").

Regarding claim 8, the combination of Kadyk and Crosbie disclosed the method of claim 1.

Kadyk did not explicitly disclose but Le disclosed that communication within the internal network is in accord with an IPv6 compatible Internet Protocol (IP) (Le, [0014] discloses that the architecture as illustrated in FIG. 1 has been recently adopted in 3GPP for the internetworking of IPv6 and IPv4 domains; In 3GPP, it is inherent that the internal network uses IPv6).

One of ordinary skill in the art would have been motivated to combine Kadyk and Le because both disclosed using a firewall to secure communications between devices in two networks (Kadyk, Fig. 4; Le, Fig. 2).

Therefore, it would have been obviousness for one of ordinary skill to integrate Le's teaching of supporting IPv6 into Kadyk such that Kadyk's system supports IPv6, as IPv6 is the trend for Internet, especially for mobile networks. The combination would have made Kadyk's invention more readily available for mobile networks that runs on IPv4.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHIRLEY X. ZHANG whose telephone number is (571)270-5012. The examiner can normally be reached on Monday through Friday 7:30am - 5:00pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Vaughn can be reached on (571) 272-3922. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S.X.Z./
Art Unit 2444
9/17/2009
/William C. Vaughn, Jr./

Supervisory Patent Examiner, Art Unit 2444